NOVALPINA CAPITAL

15 May 2019

Amnesty International
Access Now
Citizen Lab
Committee to Protect Journalists
Human Rights Watch
Privacy International
R3D: Red en Defensa de los Derechos Digitales
Reporters Without Borders
Robert L. Bernstein Institute for Human Rights, NYU School of Law and Global Justice Clinic, NYU School of Law

Response to Open Letter to Novalpina Capital on 15 April 2019

We write in response to your second open letter to Novalpina Capital on 15 April 2019 and to the open letter from Citizen Lab (now included in this public correspondence) on 6 March 2019. We have taken the time over the past weeks to prepare a detailed response reflecting the depth of our commitment to a productive dialogue with you regarding the points raised in your previous letters.

We would like to thank you for your constructive response to our previous reply on 1 March 2019. We welcome your support for our commitment to ensure NSO operates in accordance with the UN Guiding Principles on Business and Human Rights. We underline again the strength of that commitment. We are determined to do whatever is necessary to ensure that NSO technology is used for the purpose for which it is intended – the prevention of harm to fundamental human rights arising from terrorism and serious crime – and not abused in a manner that undermines other equally fundamental human rights.

The purpose of this letter is to address the points that you have raised to the extent possible and permissible at this stage. We hope that once you have considered the information and insights we provide below, you will agree to a meeting at some point in the near future at which we would then provide you with a more detailed update on the status of work underway or completed by that point.

Highly targeted interception technologies play a critical role in protecting the public. They can do so without undermining the right to privacy (ICCPR Article 17) and freedom of opinion and expression (ICCPR Article 19) when their use is prescribed by law, under circumstances that are

strictly necessary to meet the legitimate aims of a lawfully authorised body, and that are deployed in a manner that is proportionate to that aim. On the basis of your previous letter, you appear to share this perspective, which is welcome.

There can be no doubt whatsoever that the lawful, appropriate and responsible deployment of NSO technology by intelligence and law enforcement agencies is essential in order to address the serious challenges in many countries of what would otherwise be untraceable and undisruptable serious crime, terrorism, paedophile rings, human trafficking, drug cartels and the like.

As the UK National Crime Agency notes in its *National Strategic Assessment of Serious and Organised Crime 2019* report:

"Advancing technology gives offenders new tools to commit and hide their crimes. Today's criminals can sell drugs, share indecent images of children, or hack into national infrastructure from anywhere in the world, communicating covertly through encrypted services and moving illicit finances at speed. Serious and organised criminals at all levels remain engaged in the widespread abuse of encryption tools to evade law enforcement. [Serious organised crime] offenders continue to exploit both legitimate, widely commercially available encrypted communications applications, and secure encrypted platforms designed for criminal use."

We also note the contents of the affidavit recently submitted to the Israeli government by Amnesty International in order to seek the revocation of NSO's Israeli export licence. Revocation of the company's export licence would either merely create a space to be filled by alternative suppliers (none of whom – unlike Novalpina Capital – have expressed any interest in ensuring compliance with the UN Guiding Principles) or potentially deprive legitimate intelligence and law enforcement agencies of technologies that play a critical role in public safety.

It would be helpful to understand Amnesty International's intentions in pursuing this course of action given our publicly stated desire to involve them (and all of the signatories to your letter) directly in seeking to address the kind of concerns identified in the affidavit. The matters highlighted by Amnesty International reflect precisely the reasons why we believe so strongly in the merits of bringing NSO into full compliance with the UN Guiding Principles, and why we have sought to engage with all of the signatories to your letter to seek your guidance and insights. For example, as we stated in our previous reply, the revised governance framework for NSO will include enhancements to existing processes designed to mitigate the risk of misuse (as per s.29 and s.30 of the affidavit) which would be applied within a rigorous and continuous human rights due diligence programme (as per s.40 of the affidavit).

Our intention is to establish a new benchmark for transparency and respect for human rights in full compliance with the UN Guiding Principles. This will be underpinned by ongoing and meaningful consultation with affected stakeholders, and by a new model of public transparency (limited only by legal requirements and legitimate commercial confidentiality constraints). This is a challenging goal – wholly without precedent within the cybersecurity industry (in fact, it remains rare in *any* industry) – that will need to address complex matters of national security law and of intelligence and law enforcement agency practice. The intended outcome is a significant enhancement of respect for human rights to be built into NSO's policies and procedures and into the products sold under licence to intelligence and law enforcement agencies. We emphasise

again that your insights will be very important. Achievement of this goal – which we hope aligns with your own objectives – will materially benefit from your direct engagement over the coming months.

In this letter, we seek to address each of the four issues you have identified in your reply and the related concerns raised by Citizen Lab in their letter on 6 March 2019. We also comment on the points you raised in your Appendix. Finally, we provide an overview of the immediate actions now underway or planned in the near future, many of which are relevant to the points you make in your letter and Appendix.

The four issues raised in your letter

Acquisition details

The transaction has now closed. We are therefore able to provide more detail regarding the company's structure and management team than was the case when we last wrote to you.

Novalpina Capital has control of the Board of NSO. We own approximately two-thirds of the holding company of NSO (Square 2 S.a.r.l.) and have appointed the majority of Board Directors. Novalpina appointees are:

- Mickael Betito (Novalpina Capital);
- Zamir Dahbash (Shalom Tel Aviv);
- Stefan Kowski (Novalpina Capital);
- Stephen Peel (Novalpina Capital);
- Günter Schmid (KERBEROS Compliance); and
- Gerhard Schmidt (Weil).

The management and founder representatives are Shalev Hulio (NSO Chief Executive Officer and Co-Founder) and Omri Lavie (NSO Co-Founder), and the key members of the NSO executive leadership team are currently Shalev Hulio (Chief Executive Officer), Nachum Falek (Chief Financial Officer) and Kevin Wilson (General Counsel).

You also requested additional details of NSO's governance processes and operating procedures beyond the initial outline we provided in our previous letter.

We would make two points in response to that request.

The first is that there are significant constraints on lawful disclosure under the Israeli export licence regime. We attach as an Appendix to this letter an independent legal opinion requested from the Israeli law firm Herzog, Fox & Neeman regarding the extent to which information relating to regulated defence exports can lawfully be shared with third parties. As you will see from that independent legal opinion, NSO cannot legally disclose certain categories of information that you seek regarding its current operating arrangements.

Second, we would emphasise again that all of those current arrangements will be reviewed in depth over the coming months and, where required, the company's policies and procedures will be redesigned to ensure alignment with the UN Guiding Principles. We offer you the opportunity to contribute directly to that redesign process, and will therein share with you such information as is feasible within the bounds of the law and commercial confidentiality.

Statement regarding targeting of civil society

We abhor any form of misuse of any form of surveillance technology by any government, agency or individual, and we particularly condemn without hesitation any such misuse directed at people who are vulnerable simply as a consequence of their commitment to report on, speak out for or defend human rights.

For the avoidance of doubt, these principled objections extend to the activities of private investigators. Novalpina Capital would not contemplate instructing or allowing private investigators to target civil society groups investigating, reporting on, or involved in legal actions against any of its business interests. NSO are equally clear that they would not tolerate or condone any such activities. That prohibition would also extend to any intermediaries or representatives acting on behalf of Novalpina or NSO.

It is also important to note that NSO does not operate its technology in its own right to target any individual or organisation. Moreover, it would never seek to do so (even if it did possess the capabilities required, which it does not) as the company clearly has no lawful interception mandate and any such action would therefore be illegal. The company's technology is designed in such a way that it can only be deployed by an intelligence or law enforcement agency to whom the technology is sold under licence. NSO has no involvement whatsoever in any end-user agency's tactical deployment decisions.

Documentation of due diligence and investigation of reports of misuse

There are two different points here, each of which we will consider separately.

First, we did not state that Citizen Lab's "conclusions or research are flawed" (as you write in your letter), nor did we "characterise Citizen Lab's research as mere supposition or guesswork" (as Citizen Lab wrote in their open letter on 6 March 2019). Those are your words, rather than ours.

Novalpina Capital's due diligence process found that NSO conducted investigations in the very limited number of cases in which the company became aware that individuals had made claims of an attempt to access their mobile device via technology that had been attributed to NSO. In almost all of these cases, the company's investigation found that either:

- the individual had not been a target of an agency licensed to use NSO technology, and reports linking NSO to the alleged misuse were incorrect; or,
- the individual had been targeted by an agency licensed to use NSO technology that had acted with due lawful authority and as part of an investigation that was consistent with its lawful mandate.

In a very small number of cases where it could not be substantiated to NSO's satisfaction that the targeting was conducted with due lawful authority or was otherwise consistent with the ethical requirements stipulated in the end-user licence agreement, the company initiated procedures to prevent the agency involved from deploying NSO technology in the future.

Novalpina Capital received sufficient assurance on these points only after extensive interviews with NSO management, including detailed discussions that drew heavily on management's access to relevant materials. The underlying information relating to such investigations is highly confidential, with disclosure explicitly prohibited under national security legislation. It is unlawful to make such information available to any individual without the appropriate security clearances; onward disclosure to civil society groups or the wider public is therefore not possible.

We reiterate that NSO's technology is not the sole commercial product available to state intelligence and law enforcement agencies for device-level lawful interception. In addition, state entities in a number of countries are widely believed to have developed similar capabilities in their own right. Ensuring accurate attribution is not simple. There are potential limitations inherent to DNS cache probing techniques that can sometimes produce incorrect research outcomes, as Citizen Lab have publicly acknowledged. For example:

- in Citizen Lab's Report 11 (https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/), it was stated that "factors such as the use of VPNs and satellite Internet connections may skew our geolocation results. Thus, the country mapping should serve as a guide for further investigation, rather than ironclad evidence of monitoring. Additionally, it is possible that unusual configurations of DNS forwarders (such as the use of consistent hashing to consult different resolvers for different domain names) could defeat our filtering techniques and introduce false positives"; and

- at the Microsoft Blue Hat 2019 conference (https://www.bluehatil.com/index), Bill Marczak of Citizen Lab pointed out during a keynote on "Offenses in Cyber Offense" (https://www.bluehatil.com/schedule) in response to a question from the moderator about a particular allegation that "we have high confidence it was NSO. Of course in this field you can't be 100% certain".

However, please do not misunderstand the nature of the caveats we explain above. In our view, the fact that certain reports of misuse did not in fact involve NSO technology does not in any way undermine the legitimacy of efforts by civil society groups to conduct their own detailed technical investigations in response to those reports. Equally, a statement of the potential for misattribution within a highly secretive sector characterised by (as we wrote in our last letter) "an asymmetry of access to reliable information" does not amount to a denigration of those efforts, which we respect and support as a vital additional line of civil society defence against the abuse of lawful interception technologies.

It was on the basis set out above that we reached the conclusion that we described in our previous reply. Please do not assume that we doubt the overall quality of the technical analysis undertaken by Citizen Lab (and other civil society groups). Equally, please do not assume that in suggesting that some research conclusions from academic and civil society investigations – conducted

without the benefit of access to the kind of confidential materials that we describe above – may not always be completely accurate, we are somehow rejecting wholesale the methodologies, rationale and purpose of the groups involved. We are not.

We understand your (and Citizen Lab's) request for further information with regards to the potential for misuse of NSO's technology. We would be interested in your views as to how we could provide you with the assurances you seek within the significant disclosure constraints referred to above, summarised in our previous reply and explained further within the independent legal opinion from Herzog, Fox & Neeman attached as an Appendix to this letter.

Those constraints prevent us from supplying you with the "concrete documentation" related to these specific instances as you request in your letter. We also cannot supply the "information on a non-confidential basis" that Citizen Lab have requested in their letter as all of the information that would be relevant to the points raised by Citizen Lab is restricted in law from publication. For the same reasons, it will also not be possible to discuss the details of the underlying technologies utilised within NSO's products.

Second, you ask a broader question with regards to the steps taken by Novalpina Capital (as opposed to NSO) "to identify and address potential and actual human rights impacts of its activities, products and services, including those of [NSO]".

As I explained to you in my first reply to you, "Novalpina Capital are a signatory to the UN Principles on Responsible Investing, and we build ESG evaluations (including from a human rights perspective) into our investment decision processes and operating practices".

We believe that trust, transparency and accountability are the foundation for long-term business success. We expect each company within our portfolio to act with integrity and in a manner that is socially responsible. Our governance framework is designed to achieve that aim. It includes a continuous ESG due diligence process that encompasses areas including anti-bribery and corruption and anti-money laundering programmes, workplace equality and labour conditions, and all aspects of respect for human rights. Whenever weaknesses or gaps in a company's ESG performance are identified, Novalpina Capital sets specific development targets which are then tracked under a range of KPIs, against which the company management team is held to account.

Several of the board directors at each company are external non-executive directors appointed by Novalpina Capital who are typically deep subject matter experts (for example, in ESG compliance) or experienced industry experts. This form of board composition is considered to be best practice among private equity investors. The external non-executive directors exercise effective oversight over ESG matters as well as financial, operational and commercial matters, and discussion of ESG-related risks is an integral part of every board meeting.

Within each board, there is a Governance, Risk and Compliance (GRC) sub-committee. The GRC committee is chaired by a subject matter expert; other members usually include the board chair and the executive director responsible for ESG compliance. The GRC committee has significant governance powers at its disposal including the right to initiate an internal audit, commission an independent investigation, exercise a veto on a particular issue and provide specific instructions to officers and management. This approach will form the baseline for the new governance

framework at NSO, with material additions over and above what we outline above to reflect the severity of the potential harm to human rights associated with misuse of the company's technology.

Public commitment to cooperate with official investigations in Mexico

Please note that NSO is prohibited in law from providing public comment at an individual country, agency or investigation level (as the independent legal opinion in the Appendix makes clear). We therefore cannot engage in a public discussion of this specific matter. It is also important to note that NSO sells its technology under licence to end-user agencies but has no involvement in the operational use of that technology.

However, we would like to provide you with the following context (and, I hope, reassurance). NSO has always cooperated with official investigations into allegations of human rights abuse on the part of an intelligence or law enforcement agency when it has been requested to do so. That commitment applies equally and without exception to investigations in all countries in which NSO technology is deployed by a local end-user agency licensed to use it. If an official body has reason to suspect that NSO technology has been misused by a licensed in-country end-user and asks for the company's assistance in establishing the facts, NSO will promptly provide all information and assistance possible within relevant legal constraints.

The Appendix to your letter

The following seeks to address the points you have raised in the Appendix to your letter.

NSO technology and governments accused of intentionally infringing human rights

Our previous reply to you presented a brief overview of the role of the Business Ethics Committee together with a summary of current NSO governance and compliance processes. In your Appendix you have identified what you believe to be a number of shortcomings within those current arrangements.

We are developing a new governance framework for NSO which will (amongst other improvements) reflect the points you raise in your Appendix, including the importance of independent oversight and civil society consultation. The framework will be grounded in a policy commitment that recognises NSO's responsibility to respect human rights, per s.16 of the UN Guiding Principles. It will commit the company to conducting human rights due diligence in order to identify adverse human rights impacts that NSO might cause (or contribute to) through its own activities, or to which it might be directly linked (per s.17). It will also embody the company's approach to the remediation of adverse human rights impacts (per s.22) – a point we will return to later in this letter.

The governance framework will reflect the importance of considering the company's business relationship with the state entities that are the end-users of its products (as per s.13 of the UN Guiding Principles), mindful of the salient human rights risks that arise in the context of the countries within which end-user agencies operate (in line with s. 17 of the UN Guiding Principles). It will also take into account the stipulation (in the commentary to s. 11 of the UN Guiding

Principles) that "business enterprises should not undermine States' abilities to meet their own human rights obligations".

Furthermore, the framework will be designed to reflect the need for particular attention to be paid to adverse human rights impacts on individuals at “heightened risk of vulnerability or marginalisation” (in line with the commentary to s.12 and s.18) which – for NSO – would include journalists, human rights defenders, and members of other civil society groups at risk of being targeted as a consequence of the legitimate exercise of their human rights. We reiterate that your direct input into the design of this framework would be welcomed.

Mexico investigation

Addressed above.

Due diligence process conducted by Novalpina Capital prior to acquisition

Our standard ESG screening process is informed by the UN Guiding Principles and by relevant sector-specific guidance. Please see the Appendix for a summary of relevant external policies and guidelines taken into account in the course of due diligence ahead of the acquisition of NSO. That process includes consideration of human rights risks, in line with s. 17 of the UN Guiding Principles. We cannot share much of the material that informed our view of the human rights risks associated with NSO for the reasons we explain earlier in this letter.

You ask why the due diligence process did not involve consultation with civil society groups in line with s.18 of the UN Guiding Principles. The UN Guiding Principles are clear on the need for human rights impacts to be assessed in the context of a merger or acquisition (as addressed above). However, when the fact that a transaction is being contemplated by either party is not in the public domain, and when all aspects of the negotiations are necessarily restricted to a small group bound under non-disclosure agreements for commercial reasons, the barriers to public consultation are considerable. In theory, members of a civil society group could be consulted during the course of confidential negotiations, but only if they were prepared to sign a non-disclosure agreement prior to engagement – a legally binding commitment that would appear to be in direct conflict with those groups’ public commitment to transparency. We have not encountered such arrangements in our experience but would welcome hearing of such examples from your collective experience.

Instead, the ESG due diligence process conducted ahead of the NSO transaction included a comprehensive analysis of all relevant public materials and research reports produced by civil society groups (including those produced by the signatories to your letter). This is in line with the suggestion in the commentary to s.18 of the Guiding Principles that a business enterprise should “consider reasonable alternatives” such as “consulting credible, independent expert resources” if direct consultations with potentially affected stakeholders are not possible .

The Appendix to this letter includes a sample list of the resources analysed. Those resources directly informed our understanding of the associated human rights risks (and, indeed, directly informed our view of the merits of building on NSO’s current governance process to bring these into alignment with the UN Guiding Principles).

We disagree with your objections to the individuals involved in the due diligence process. One is a senior partner in an international law firm with extensive experience of conducting due diligence across multiple sectors; the other has a 15-year background in international compliance and ESG matters. It is completely appropriate for a company to leverage relevant expertise among its retained external advisers (as well as within its own workforce, for that matter) in conducting human rights due diligence. In any business context, a retained external adviser or senior employee with sufficient expertise is wholly capable of providing considered and objective recommendations to the leadership of a company. It is neither reasonable nor rational to infer that a pre-existing contractual relationship with a company somehow delegitimises the analysis by, and advice from, the professionals concerned on grounds of a conflict of interest. If that were the case, there would be no point in any company retaining external advisers or building in-house expertise in any professional function.

Corporate and shareholder structure of NSO

Addressed earlier in this letter.

Mitigation of human rights risks associated with NSO technology

Addressed above. We respond to your point about the "substantiation" (your emphasis) of abuse allegations later in this letter.

Business Ethics Committee membership and deliberations

Please see our comments earlier with regard to your views on the Business Ethics Committee and our plans to bring the NSO governance framework into alignment with the UN Guiding Principles. To achieve that alignment, the composition and procedures of the current oversight mechanisms will change, as will the level of transparency involved. The new governance arrangements will be shaped to a significant extent through meaningful civil society consultation, as per s.18 (and also in the design of any grievance and remedy process as per s.31), and again we would welcome your involvement.

Private investigators targeting civil society groups

Addressed earlier in this letter.

Export licence details

There are mandatory and significant disclosure restrictions imposed under many countries' export licensing regimes. The independent legal opinion that we attach as an Appendix to this letter provides an overview of the boundaries of what can lawfully be published. Our commitment – through the planned NSO transparency framework – is to disclose all information where it is legally safe to do, that does not risk public safety or put employees at risk of harm, and that does not breach legitimate commercial confidentiality constraints – all of which is in line with s.21 of the UN Guiding Principles. That framework will encompass all aspects of the export licence regimes in all countries where these apply. It will also encompass the full range of NSO's products.

Monitoring and enforcing compliance with end-user agreements to prevent misuse

As you will see from the attached independent legal opinion, there are significant lawful disclosure constraints regarding many aspects of the company's operations. Additionally, other relevant information that you seek – such as details of end-user agreements and enforcement of terms and conditions – is confidential under NSO's current governance and disclosure policies and therefore cannot be shared at this time.

I would emphasise, though, that this is the status quo today. To reiterate, the transparency framework we are developing for NSO will be based on a default assumption that all that can be disclosed will be disclosed when necessary to ensure that stakeholders (including civil society groups and the public as a whole) are appropriately informed and aware of the company's activities (subject, however, to the range of constraints explained elsewhere in this letter).

We would also draw your attention to our comments earlier in this letter regarding our intention to ensure that the new governance framework for NSO includes a particular focus on the protection of vulnerable groups, in line with s.12 and s.18 of the UN Guiding Principles.

Substantiation and the threshold for action in response to human rights risk

We think you are misunderstanding the context within which we used the term "substantiated" in our previous reply to you. NSO will investigate any report of misuse whenever:

- that report relates to the activities of an intelligence or law enforcement agency that has been granted an end-user licence to operate NSO technology; and
- the nature of the misuse involved would appear to imply the deployment of a capability that NSO provides (regardless of whether the specific product used was provided by NSO or a third party).

The misuse does *not* have to be substantiated as a precondition for NSO deciding to investigate, nor must the report of the misuse be in the public domain. There is, in effect, an automatic presumption of the requirement to investigate a report in *any* instance in which it is feasible that NSO technology may have been used in breach of the end-user licence conditions.

The reference to "substantiated" in our previous reply to you relates to instances of suspected misuse that have been investigated by NSO and – at the conclusion of that investigation – are found to be a breach of the end-user licence conditions. That conclusion does not rely on an investigation outcome of 100% certainty; it is formed on the basis of a balance of probabilities. If NSO believes after investigation that it is more likely than not that an end-user has misused the technology, the company will take action.

For the reasons outlined earlier in this letter, we are unable to provide you with the details of the circumstances under which specific contracts have been terminated, but we reiterate that the company has indeed terminated contracts based on the outcome of such investigations.

We are certainly not proposing – as you appear to suggest in your references to s.22 of the UN Guiding Principles – that individuals who believe their fundamental rights have been harmed as a

consequence of an agency's deployment of NSO technology should not expect access to a grievance and remedy process until and unless that harm is substantiated. There is an important distinction between a publicly communicated and transparent grievance process – under which affected stakeholders can raise concerns and trigger investigation – and the remedy process that should then follow if an investigation concludes that human rights harms have occurred. The points you raise in your letter appear to elide that distinction.

We also understand fully the importance of an effective process for remedy at the point at which a specific grievance (or a specific concern about a potential harm to fundamental rights, even without such harm having arisen) is demonstrated through investigation and analysis to be well-founded.

One of the factors that will need to be considered carefully when designing that remedy process is that it is the state entities deploying technology supplied by NSO (i.e. national intelligence and law enforcement agencies) – not NSO itself – who are the primary actors in any potential harm to fundamental rights, and that similarly under the UN Guiding Principles it is the state that bears primary responsibility for remedy. The remedy process under the new NSO governance framework will therefore need to be complementary to – and facilitate – a broader process of remediation by the state in cases of misuse. This is a complex area that will require direct input from civil society groups to achieve the optimum outcome, in accordance with s.31 of the UN Guiding Principles.

Our next steps

Between now and the summer, we will progress our work on NSO's governance and transparency frameworks.

We have commissioned internationally recognised and leading external experts in the field of human rights to prepare an independent report on the effectiveness of NSO's current governance framework. This work will involve direct engagement with civil society groups, and we invite the signatories to your letter (and any other interested parties) to participate. The independent report will explore the key themes raised in your letters as necessary inputs to ensure that the assessment and recommendations for action are as comprehensive as possible.

As part of a new governance and transparency framework, NSO will in future aim to disclose all information of relevance and importance to civil society groups unless it is expressly prohibited in law from doing so or it cannot do so for reasons of public safety, risk of employee harm or to protect legitimate commercial confidentiality. The independent legal opinion attached to this letter will help inform our understanding of the parameters of this disclosure. Again, we invite you to engage with us over the coming months to help shape the outcome.

We will also conclude a benchmarking exercise to establish current models of best practice in governance and transparency across relevant sectors (cybersecurity, defence, telecommunications, technology) that will inform the outline of the new governance and transparency frameworks for NSO. We have engaged experienced legal counsel to advise us on the design of these frameworks, supported by additional external specialists with a background in corporate transparency in a human rights context.

As explained above, we are committed to meaningful consultation with affected stakeholder groups and other members of civil society with a direct interest in NSO's activities, and we would welcome active engagement with all of the signatories to your letter.

Yours sincerely,

Stephen Peel
Founding Partner
Novalpina Capital

Cc:
Stefan Kowski – Founding Partner, Novalpina Capital
Bastian Lueken – Founding Partner, Novalpina Capital
Shalev Hulio – Chief Executive Officer and Founder, NSO

Appendix

1. The Novalpina Capital ESG screening process

There is no single generally accepted standard under which a potential transaction is assessed for ESG screening purposes. Novalpina Capital is committed to ensuring the highest level of ESG assessment in the global private equity industry. To achieve this, we have reflected the following in devising our approach:

- the Principles For Responsible Investment ("PRI"), an investor initiative in partnership with the UNEP Finance Initiative and the UN Global Compact;
- the UN Guiding Principles on Business and Human Rights;
- the European Commission ICT Sector Best Practice Guide on Implementing the UN Guiding Principles on Business and Human Rights;
- the Human Rights Impact Assessment Guidance and Toolbox issued by the Danish Institute for Human Rights;
- UK Government guidance on Assessing Cyber Security Export Risks in Human Rights/National Security;
- ESG-related advice from the Private Equity Growth Capital Council ("PEGCC", now the American Investment Council); and
- comparable corporate ESG risk management programmes (e.g. Nokia, Nestlé, Shell plus relevant companies in the defence sector).

2. Sample list of selected external resources analysed in the course of the Novalpina Capital ESG assessment

- https://www.amnesty.org/en/latest/news/2018/08/is-nso-group-a-goto-company-for-human-rights-abusers/
- https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/
- https://www.amnesty.org/en/latest/news/2018/08/staff-targeted-with-malicious-spyware/
- https://www.amnesty.org/en/latest/news/2018/11/israelroguenso-group-must-have-licence-revoked-over-controversial-surveillance-software/
- https://www.amnesty.org/en/latest/news/2017/05/the-guy-who-saved-your-iphone-from-hackers-is-stuck-in-a-uae-jail/
- https://www.accessnow.org/eu-member-states-are-watering-down-spyware-regulation/
- https://www.accessnow.org/saving-free-expression-in-mena-what-happens-after-khashoggis-death/
- https://www.accessnow.org/european-parliament-fighting-strengthen-rules-surveillance-trade/
- https://www.accessnow.org/nso-group-surveillance-tech-shadows-francisco-partners/
- https://www.accessnow.org/blackstone-wont-invest-nso-groups-toxic-spyware/
- https://www.accessnow.org/victims-nso-group-malware-attacks-deserve-silence-complicity/
- https://www.accessnow.org/nso-group-responds-human-rights-violations-comes-short/

- https://www.accessnow.org/blackstone-hit-brakes-nso-spyware-deal/
- https://www.accessnow.org/access-now-united-nations-spyware-uae-surveillance-france-shutdowns-africa/
- https://www.accessnow.org/international-groups-reject-mexican-government-surveillance-public-health-advocates/
- https://www.apnews.com/ca8d2394c1694bbcac85744dab5cc5bf
- https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/
- https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/
- https://citizenlab.ca/2018/11/open-letter-to-francisco-partners-continued-misuse-of-nso-groups-pegasus-technology/
- https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/
- https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
- https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/
- https://citizenlab.ca/2018/05/open-letter-to-francisco-partners-request-for-follow-up-on-apparent-misuse-of-sandvine-technology-and-sale-of-nso-group-to-verint-systems/
- https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/
- https://citizenlab.ca/2017/08/reported-blackstone-nso-deal-failure-risks-investing-spyware-companies/
- https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/
- https://citizenlab.ca/2017/07/open-letter-to-blackstone-possible-nso-acquisition/
- https://citizenlab.ca/2017/07/mexico-disappearances-nso/
- https://citizenlab.ca/2017/06/more-mexican-nso-targets/
- https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/
- https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/
- https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
- https://edition.cnn.com/2019/01/12/middleeast/khashoggi-phone-malware-intl/index.html
- https://www.haaretz.com/israel-news/.premium-apparent-sale-of-nso-highlights-dark-side-of-israeli-cybertechnology-1.6133821
- https://www.hrw.org/news/2017/12/06/ethiopia-new-spate-abusive-surveillance
- https://www.hrw.org/news/2017/09/08/human-rights-watch-submission-re-human-rights-defenders-and-civic-space-context
- https://www.hrw.org/news/2017/06/20/mexico-investigate-spyware-attack
- https://www.jpost.com/printarticle.aspx?id=573419
- http://www.law.nyu.edu/sites/default/files/Bernstein%20Institute%20Conference%20Digest.pdf
- https://www.miamiherald.com/news/nation-world/national/article222789710.html
- https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html
- https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html

- https://www.nytimes.com/2019/01/28/world/black-cube-nso-citizen-lab-intelligence.html
- https://privacyinternational.org/press-release/2656/privacy-international-aclu-demand-government-disclose-nature-and-extent-hacking
- https://privacyinternational.org/state-privacy/1006/state-privacy-mexico
- https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon
- https://privacyinternational.org/legal-action/us-hacking-foia
- https://privacyinternational.org/blog/2279/shining-light-federal-law-enforcements-use-computer-hacking-tools
- http://privacyinternational.org/examples-abuse/2604/nso-group-pegasus-spyware-found-operating-45-countries
- https://privacyinternational.org/examples-abuse/2605/lawsuits-target-nso-group-selling-spyware-governments-targeting-activists-and
- https://privacyinternational.org/feature/2225/open-source-guide-researching-surveillance-transfers
- https://privacyinternational.org/feature/811/monitoring-surveillance-industry-using-data-protect-privacy
- https://privacyinternational.org/advocacy-briefing/994/letter-and-briefing-human-rights-implications-reported-mexican-government
- https://r3d.mx/2019/01/28/investigadores-de-citizen-lab-fueron-objetivo-de-operacion-encubierta-por-su-labor-sobre-nso-group/
- https://r3d.mx/2018/08/31/nso-group-es-demandada-ante-tribunales-de-israel-y-chipre-por-negligencia-y-complicidad-en-el-caso-en-el-caso-gobiernoespia/
- https://r3d.mx/2018/05/31/ahmed-mansoor-es-sentenciado-a-10-anos-de-prision-en-los-eau/
- https://r3d.mx/2017/10/30/nso-group-se-arrepiente-de-haberle-vendido-pegasus-al-gobierno-mexicano/
- https://r3d.mx/2017/08/16/blackstone-ya-no-invertira-en-nso-group/
- https://r3d.mx/2017/08/01/organizaciones-enviamos-carta-a-blackstone-group-sobre-posible-inversion-en-nso-group/
- https://r3d.mx/2017/06/21/posicionamiento-frente-a-espionaje-de-personas-defensoras-de-derechos-humanos-periodistas-y-activistas-anticorrupcion/
- https://r3d.mx/2017/06/21/gobierno-espia-la-vigilancia-sistematica-en-contra-de-periodistas-y-defensores-de-derechos-humanos-en-mexico/
- https://r3d.mx/2017/05/12/ahmed-mansoor-el-activista-que-ayudo-a-descubrir-el-malware-pegasus-esta-encarcelado/
- https://r3d.mx/proyecto/espionaje-nso/
- https://r3d.mx/2017/02/14/organizaciones-de-la-sociedad-civil-rechazamos-espionaje-gubernamental-a-defensores-del-derecho-a-la-salud-en-mexico/
- https://r3d.mx/2017/02/13/el-espionaje-del-gobierno-de-mexico-contra-defensores-del-derecho-a-la-salud-no-debe-quedar-impune-osc/
- https://r3d.mx/2016/06/01/conoce-a-una-victima-del-crecimiento-masivo-del-software-para-espionaje/
- https://rsf.org/en/news/mexican-journalists-targeted-pegasus-spyware
- https://rsf.org/en/reports/dubious-lucrative-surveillance-business
- https://www.washingtonpost.com/opinions/2018/12/12/washington-must-wake-up-abuse-software-that-kills/?tid=ss_mail&utm_term=.a342bbeaca7d

- https://www.washingtonpost.com/outlook/2019/01/17/how-us-surveillance-technology-is-propping-up-authoritarian-regimes/?utm_term=.7c8a70dea0fe

3. Herzog, Fox & Neeman (HFN) independent legal opinion

Please see next page.

HERZOG FOX & NEEMAN
LAW OFFICE

May 13, 2019

File: 44170

To: Stephen Peel, Novalpina Capital

From: Daniel Reisner, HFN

Subject: **Access to information relating to regulated exports under Israeli law**

A. Introduction

1. I have been requested to advise on the legal rules and limitations in Israel applicable to the sharing of information relating to regulated defence exports.

2. More specifically, I have been asked what information relating to such exports can be shared with third parties, and especially non-Israeli third parties.

B. Experience and expertise

3. My name is Daniel Reisner. I have been a lawyer and member of the Israeli bar for over 30 years.

4. Following a lengthy career as a senior government lawyer, for the last 11 years I have been a partner at the Israeli law firm of Herzog, Fox & Neeman (HFN), where I chair the firm's international law, defense national security and international trade practice groups.

5. Today, my department is widely viewed as the leading practice group in Israel in the field of export controls. Our clients include almost all of the prominent Israeli defense, homeland security and cyber companies as well as many of the leading multinationals in these fields.

C. Introduction to Israeli Defense Export Control Laws

6. Similar to most other western countries, Israel has two separate export control regimes – a defence export control regime, and a civilian export control regime.

7. The defence export control regime is administered by the Ministry of Defence's (MOD) Defence Export Control Agency (DECA) under the 2007 Defence Export Control Law (DECL)[1]. This regime primarily focuses on items, services and knowhow appearing on the MOD's Combat Equipment List[2] (similar to the Munitions List common in many western countries). In addition, DECA is also responsible for the administration of dual-use exports (as defined in the Wassenaar Arrangement Dual-Use List), provided that either the end use or the end user of such exports are defence or security related.

8. The civilian export control regime is administered by the Ministry of Economy ("MOE"), and is primarily focused on dual use exports not intended for security or defence end users or end uses.

9. For the purposes of this memorandum, and due to the fact that all of NSO's current product line in Israel falls under the defence export control regime, I have been asked to focus solely on this regime, as administered by DECA.

10. The DECA export control regime is relatively unique in that it includes a four-stage export licensing process:

    a. Every potential defence exporter is first required to register in the DECA administered Defence Exporters Registry;

---

[1] A copy of which can be found at http://www.exportctrl.mod.gov.il/English/Pages/Defense-Export-Control-Law-.aspx.

[2] Available at http://www.exportctrl.mod.gov.il/Documents/%D7%97%D7%95%D7%A7%20%D7%94%D7%A4%D7%99%D7%A7%D7%95%D7%97%20+%20%D7%A6%D7%95%D7%95%D7%99%D7%9D%20+%20%D7%AA%D7%A7%D7%A0%D7%95%D7%AA/tsav-pikuah-tsiyud-lehima.pdf (Hebrew only).

b. Once a company or an individual has been duly registered, they are then required to register with DECA all controlled products, services or knowhow which they may wish to export;
c. Only after both the above steps have been completed, the company or individual may apply for a Marketing License, which is generally required before they may conduct any marketing activities for regulated goods, services or knowhow. A marketing license covers all marketing activities, from the initial meetings with potential customers, up to and including signing a binding contract;
d. Finally, before any items, services or knowhow can be physically exported from Israel to another country (or to a non-Israeli in Israel), an Export License must be sought and received from DECA.

D. Confidentiality of DECA Licenses

11. As part of their registration process (stage 2 referred to in Section 10(b) above), all controlled products, services and knowhow are granted a security classification by the MOD[3]. Such classifications range from "unclassified", "confidential" and "secret", and up to the highest classification of "top secret".

12. DECA licenses (both marketing and export) are similarly classified, using the same classification levels. The MOD decides on the specific license classification as a function of the classification of the relevant products, services and knowhow; the sensitivity of the customer country; and the overall sensitivity of the project in question.

13. In the event that a license has been classified as "confidential" or higher, all of its contents would be deemed as "secret information" under Israeli law. Consequently, providing any such information to an unauthorized third party (Israeli or otherwise) would be a violation of Section 113 of the Israeli 1977 Penal Law (the Israeli equivalent to the Official Secrets Act in the UK) and could lead to criminal proceedings.

[3] See DECA's explanation of this process on their website at http://www.exportctrl.mod.gov.il/Guide/Pages/Step3.aspx (Hebrew only).

14. However, and possibly counter-intuitively, the fact that a specific license has been deemed by DECA to be "unclassified" does not mean that its contents may be shared with third parties.

15. On the contrary, DECA constantly emphasizes to Israeli defence exporters that it is totally prohibited to share any DECA license (irrespective of classification), or any information relating to any such license, with any third party, without the express written and prior authorization of DECA.

16. This requirement is usually specifically included in the DECA licenses and product registration documents (I cannot attach an example, for the obvious reason that doing so would, in itself, be a violation of said rule).

17. In addition, DECA representatives repeatedly stress this policy requirement in training sessions provided to defence exporters. It also used to appear prominently in the FAQ section of DECA's previous website, but has yet to re-appear on the new DECA website (although we have no basis to believe that this represents a policy change in this context).

18. Additionally, we are aware of several cases (the details of which we are not at liberty to discuss) in which this DECA license confidentiality requirement was invoked in the context of international investigations and court proceedings, resultantly preventing any disclosure of information relating to defence exports, including details relating to DECA licenses.

19. We have also been involved in several other cases in which this same confidentiality requirement prevented us from divulging licensing details to Israeli banks, who required such information for the purpose of AML verifications relating to defence export transactions.

20. Rather exceptionally, in September 2018 Israeli media published a recent decision of the Tel Aviv District Court, in which it was decided to accept the MOD's position to refuse a freedom of information request to make public information relating to the security cooperation between Israel and Sri Lanka between the years 2002 and 2011.

21. The court's decision in this regard (which was originally not made public due to a temporary gag order) referred to the fact that the information sought included, *inter alia,* information relating to export transactions with this country. The court explained that publishing the information sought (in violation of the secrecy agreement between the two states) would have problematic consequences for Israel's relations with other countries[4].

22. This case is quite unique, in that normally such proceedings would remain outside of public sight as a result of permanent gag orders issued by the courts at the request of the MOD. However, it is quite indicative of the MOD's consistent policy that any publication of details relating to Israeli defence exports is prejudicial to Israel's national security and foreign relations.

23. It should be clarified that any perceived violation by an Israeli defence exporter of this DECA licensing confidentiality requirement could result in serious consequences, ranging from temporary or permanent revocation of licenses and registration, monetary fines, or even (in extreme cases) the initiation of criminal proceedings.

24. I can further attest that the DECA leadership has recently personally reconfirmed to me, in a face to face meeting, their strict expectation of full compliance with this requirement by all registered defence exporters.

25. To exemplify the extremes to which the MOD has gone to protect what it perceives to be sensitive information relating to Israel's defence exports policies – DECA has developed a list of (currently) 101 jurisdictions, for which a marketing license will no longer be required with respect to most products (although the requirement of an export license remains intact).

---

[4] See https://jacobinmag.com/2018/11/israel-arms-sales-eitay-mack-idf, which provides an in-depth analysis (from the perspective of a human rights activist) of the Israeli government's non disclosure policies relating to defence exports, including reference to the recent Tel Aviv District Court decision.

26. While this has been widely viewed as a step towards easing Israel's otherwise highly onerous export control requirements, the actual list of the 101 jurisdictions is not public, and is only made available to registered defence exporters, on condition that they formally undertake not to share it with third parties.

27. In other words, only companies which have been licensed by DECA can learn which jurisdictions do not require a marketing license. Once again – this is the result of the extremely high sensitivity attributed in Israel to the government's export policies.

E. Analysis and conclusions

28. I have been asked what information relating to controlled Israeli defence exports, including details concerning related licenses, can be shared with third parties, and especially non-Israeli third parties.

29. On the basis of the MOD rules and policies outlined above, as well as our extensive experience in dealing with such matters, I can state that it is strictly prohibited for any Israeli defence exporter to share information relating to any licenses received from the MOD with respect to controlled defence exports.

30. This prohibition is wide in scope, and would cover not only specific details appearing in the licenses (such as customer information; product information; value; license terms, conditions and limitations etc.) but also more general information, including the number of licenses issued (or refused) and the names of customer countries (or countries refused for licenses).

31. While generally applicable to all third parties, the above would especially apply with regard to any non-Israeli entity or individual, whether in Israel or abroad.

32. Consequently, in any instance in which there arises a need (or interest) to share information relating to DECA licenses with a non-Israeli third party, we would first need to approach DECA in this regard, and seek their guidance and permission (which would usually not be easily forthcoming). Doing otherwise could result in serious potential consequences, for involved companies and individuals alike.

Daniel Reisner

Herzog, Fox & Neeman